How the UK passed the most invasive surveillance law in democratic history

verfassungsblog.de/how-the-uk-passed-the-most-invasive-surveillance-law-in-democratic-history/

Paul Bernal Fr 25 Nov 2016

Fr 25 Nov 2016

You might not have noticed thanks to world events, but the UK parliament recently approved the government's so-called Snooper's Charter and it will soon become law. This nickname for the Investigatory Powers Bill is well earned. It represents a new level and nature of surveillance that goes beyond anything previously set out in law in a democratic society. It is not a modernisation of existing law, but something qualitatively different, something that intrudes upon every UK citizen's life in a way that would even a decade ago have been inconceivable.

The bill requires internet and telecoms companies to keep records of every website or app we use and all our phone calls and messages for 12 months. It leaves us in the unenviable position of leading the world in the legalisation of surveillance. And it will likely be used by more authoritarian regimes around the globe as evidence that mass surveillance, online hacking and encryption backdoors are perfectly fine.

Because of the way we now use the internet for almost every element of our lives, this is not like a few carefully chosen wiretaps on suspects. It's granting the authorities the capacity to spy on pretty much everything done by pretty much everyone. And yet we have let this law pass with very few headlines and barely a breath of resistance from our politicians.

There are still some legal avenues to prevent it from coming into effect, most directly through the European Court of Justice (while the UK is still in the EU) and the European Court of Human Rights (which is separate from the EU). But more likely to be our saving graces are the inherent problems with implementing this poorly conceived legislation and the constantly developing technology that can potentially by-pass the law.

A well scrutinised bill?

The Home Office may well say that it has been one of the most highly scrutinised and analysed bills in recent history. And on the face of it, they would be right. The UK's surveillance activities have been the subject of a long series of reviews by a wide range of bodies. What the Home Office won't say is that they have responded to these various reviews with a mixture of sidestepping, ignoring, refusing and paying lip-service to their recommendations.

For example, the Intelligence and Security Committee's recommendation that "privacy protections should form the backbone of the draft legislation, around which the exceptional powers are then built" was responded to by changing one title from "General Protections" to "General Privacy Protections".

The bill itself remains substantially identical to the one that was initially proposed and was highly criticised by many of the reviews. There are limits built in – such as the need for a judge and the home secretary to sign off warrants to intercept communication – but whether they will be more than a rubber stamp is questionable and will need to be carefully watched.

Most of those in parliament who knew how bad this was allowed themselves to be distracted. Conservative MP and civil rights campaigner David Davis was seduced by his new role as Brexit secretary. Labour deputy leader Tom Watson was focused on the conflict within the Labour Party. And former Liberty director Shami Chakrabarti was seduced by a peerage and the allure of a Shadow Cabinet role.

Quite why those who should have known better – in particular, Jeremy Corbyn and shadow home secretary Diane Abbott who have been the subject of inappropriate and politically motivated surveillance themselves – waved it through remains a mystery. The only real resistance came from what is left of the Lib Dems, the SNP and Green MP Caroline Lucas. It wasn't nearly enough.

In the end, parliament failed through a combination of incomprehension and political cowardice. After all, who wants to be seen to prevent something that might save us all from a terrorist attack? Aside from this, the House of Commons was preoccupied with issues that were well established, such as protection for journalists, or staring them in the face, such as the confidentiality of their own communications.

That meant that they missed both the nature of the new style of surveillance and its impact on people's lives. The biggest issues, such as the impact of mass hacking, were missed entirely or fundamentally misunderstood. For example, the data that will be gathered – known as "internet connection records" — was characterised as the equivalent of an itemised phone bill for the internet. In reality, it's a record of our movements, interests, friends, health, sexual preferences and even our tastes in music. And even more information about us could be derived from that data.

Saving graces?

Legal challenges to the bill at the European courts of justice and human rights are certain to happen and quite likely to succeed. The courts have a strong recent track record of finding this level of intrusion incompatible with fundamental rights. Although, in the current anti-European climate, it is equally likely that the courts will be largely ignored by the UK government.

That leaves a technological solution, and here lies both the route around the bill and its fundamental problem. Some of the worst parts of the bill –- the internet connection records in particular -– will be both difficult and extremely costly to implement, and may take years. Technologically able people will find ways to bypass the bill. The use of encryption and anonymisation will increase in response to the clampdown, as will other ways to avoid being tracked and then tracked down. That includes most of the "bad guys" that are ostensibly the targets of this legislation.

As David Davis said, before being distracted by Brexit, this kind of surveillance will only catch the innocent and the incompetent. The innocent should not be caught and the incompetent can be caught any number of ways.

What this surveillance is good for is monitoring entire populations for social control: monitoring naïve opposition groups, shutting down popular protests or dissidence, and political manipulation. In a world where Donald Trump can be elected President of the United States this is something that should disturb us greatly.

This article has been previously posted on The Conversation and is republished here with kind permission by the author.

SUGGESTED CITATION Bernal, Paul: *How the UK passed the most invasive surveillance law in democratic history, VerfBlog,* 2016/11/25, http://verfassungsblog.de/how-the-uk-passed-the-most-invasive-surveillance-law-in-democratic-history/.